

NEW EXTREMAL BINARY SELF-DUAL CODES OF LENGTHS 66 AND 68 FROM CODES OVER $R_{k,m}$

ABİDİN KAYA AND NESİBE TÜFEKÇİ

ABSTRACT. In this work, four circulant and quadratic double circulant (QDC) constructions are applied to the family of the rings $R_{k,m}$. Self-dual binary codes are obtained as the Gray images of self-dual QDC codes over $R_{k,m}$. Extremal binary self-dual codes of length 64 are obtained as Gray images of λ -four circulant codes over $R_{2,1}$ and $R_{2,2}$. Extremal binary self-dual codes of lengths 66 and 68 are constructed by applying extension theorems to the \mathbb{F}_2 and $R_{2,1}$ images of these codes. More precisely, 11 new codes of length 66 and 39 new codes of length 68 are discovered. The codes with these weight enumerators are constructed for the first time in literature. The results are tabulated.

1. INTRODUCTION

An interesting family of linear codes are self-dual codes. Self-dual codes over finite fields have been studied extensively. Some good binary codes such as the extended binary Golay code and the extended quadratic residue codes of parameters $[48, 24, 12]_2$ and $[104, 52, 20]_2$ are of this type. Such codes have also attracted a lot of attention due to their connections to design theory.

Conway and Sloane gave an upper bound for the minimum distance of a binary self-dual code in [4]. The bound was finalized in [17] as follows; the minimum distance d of a binary self-dual code of length n satisfies $d \leq 4 \lfloor n/24 \rfloor + 6$ if $n \equiv 22 \pmod{24}$ and $d \leq 4 \lfloor n/24 \rfloor + 4$, otherwise. A self-dual code meeting this bound is called *extremal*. The possible weight enumerators of extremal self-dual binary codes of lengths up to 64 and 72 were determined in [4]. Since then, constructing new extremal binary self-dual codes have been an attractive research area. Different techniques such as circulant constructions, automorphism groups and extensions are used to obtain new extremal binary self-dual codes. For some of the works done in this direction we refer the reader to [5, 12, 20, 22].

Recently, some rings of characteristic 2 have been used effectively to construct new extremal binary self-dual codes. Lifts were used in [11] and [13]. Extension theorems for self-dual codes were applied to codes over $\mathbb{F}_4 + u\mathbb{F}_4$ in [16]. Karadeniz et al. used four circulant construction over $\mathbb{F}_2 + u\mathbb{F}_2$ in [9].

In this work, we give a generalization of four circulant construction and combine the lifting and extending methods. The computational algebra system MAGMA [2] is used for the results. The rest of the paper is organized as follows: Section 2 consists of preliminaries about the family of rings $R_{k,m}$ and codes over these. In

2010 *Mathematics Subject Classification.* Primary 94B05, 94B60, 94B65.

Key words and phrases. extremal codes, codes over rings, Gray maps, quadratic double-circulant codes.

Section 3, we introduce quadratic double circulant codes over $R_{k,m}$. Section 4 includes constructions for extremal singly-even binary self-dual codes of length 64 as Gray images of four circulant self-dual codes over $R_{2,1}$ and $R_{2,2}$. In Section 5, extremal binary self-dual codes of lengths 66 and 68 with previously unknown weight enumerators are constructed as extensions and as Gray image of extensions. More precisely, 11 new codes of length 66 and 39 new codes of length 68 are constructed.

2. PRELIMINARIES

The ring $R_{k,m}$ was introduced in [19] as a generalization of $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, which was studied in [23]. The ring is a commutative local Frobenius ring of characteristic 2 that is defined as

$$R_{k,m} = \mathbb{F}_2[u, v] / \langle u^k, v^m, uv - vu \rangle \text{ where } k \geq m \geq 1.$$

Note that $R_{2,2} = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, for more details on the structure of the ring we refer to [19].

A linear \mathcal{C} of length n over $R_{k,m}$ is an $R_{k,m}$ submodule of $R_{k,m}^n$. The dual \mathcal{C}^\perp of a linear code \mathcal{C} is defined with respect to the Euclidean inner product as

$$\mathcal{C}^\perp := \left\{ (b_1, b_2, \dots, b_n) \in R_{k,m}^n \mid \sum_{i=1}^n a_i b_i = 0, \forall (a_1, a_2, \dots, a_n) \in \mathcal{C} \right\}.$$

A code \mathcal{C} is said to be *self-orthogonal* if $\mathcal{C} \subseteq \mathcal{C}^\perp$, and *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$. A binary self-dual code is called *doubly-even* if the weight of any codeword is divisible by 4 and *singly-even* otherwise. By [21], the ring $R_{k,m}$ is suitable to study self-dual codes;

Lemma 2.1. [19] *A linear code \mathcal{C} of length n over $R_{k,m}$ satisfies $|\mathcal{C}| \cdot |\mathcal{C}^\perp| = |R_{k,m}|^n$.*

Definition 2.2. [19] Take an element $\bar{a} = \bar{a}_0 + \bar{a}_1 u + \bar{a}_2 u^2 + \dots + \bar{a}_{k-2} u^{k-2} + \bar{a}_{k-1} u^{k-1}$ of $(\mathcal{R}_{k,1})^n$, where $\bar{a}_i \in \mathbb{F}_2^n$. Then define the Gray map ϕ_{k1} from $(\mathcal{R}_{k,1})^n$ to $(\mathbb{F}_2)^{kn}$ as follows: when k is even let

$$\phi_{k1}(\bar{a}) = (\bar{a}_0 + \bar{a}_1 + \dots + \bar{a}_{k-2} + \bar{a}_{k-1}, \bar{a}_1 + \dots + \bar{a}_{k-2} + \bar{a}_{k-1}, \\ \bar{a}_1 + \dots + \bar{a}_{k-2}, \dots, \bar{a}_{\frac{k}{2}-1} + \bar{a}_{\frac{k}{2}} + \bar{a}_{\frac{k}{2}+1}, \bar{a}_{\frac{k}{2}-1} + \bar{a}_{\frac{k}{2}}, \bar{a}_{\frac{k}{2}})$$

and when k is odd let

$$\phi_{k1}(\bar{a}) = (\bar{a}_0 + \bar{a}_1 + \dots + \bar{a}_{k-2} + \bar{a}_{k-1}, \bar{a}_1 + \dots + \bar{a}_{k-2} + \bar{a}_{k-1}, \\ \bar{a}_1 + \dots + \bar{a}_{k-2}, \dots, \bar{a}_{\frac{k-3}{2}} + \bar{a}_{\frac{k-1}{2}} + \bar{a}_{\frac{k+1}{2}}, \bar{a}_{\frac{k-1}{2}} + \bar{a}_{\frac{k+1}{2}}, \bar{a}_{\frac{k+1}{2}}).$$

In [19], the Gray map is extended to $R_{k,m}$ by viewing $R_{k,m}$ as a vector space over $R_{k,1}$ basis $\{1, v, v^2, \dots, v^{m-1}\}$ as follows;

$$\phi_{km}(c) = (\phi_{k1}(\sum_{i=0}^{m-1} \bar{c}_{ki}), \phi_{k1}(\sum_{i=1}^{m-1} \bar{c}_{ki}), \phi_{k1}(\sum_{i=1}^{m-2} \bar{c}_{ki}), \\ \dots, \phi_{k1}(\sum_{i=\frac{m}{2}-1}^{\frac{m}{2}+1} \bar{c}_{ki}), \phi_{k1}(\sum_{i=\frac{m}{2}}^{\frac{m}{2}} \bar{c}_{ki}), \phi_{k1}(\sum_{i=\frac{m}{2}}^{\frac{m}{2}} \bar{c}_{ki})).$$

where $c = \sum_{0 \leq i \leq m-1} c_{ki} v^i$, $c_{ki} \in R_{k,1}$. The Lee weight w_L of an element a of $R_{k,m}$ is defined to be the Hamming weight of the Gray image. The Gray map ϕ_{km} preserves duality.

Theorem 2.3. [19] *Let \mathcal{C} be a self-dual code over $R_{k,m}$ of length n . Then $\phi_{km}(\mathcal{C})$ is a binary self-dual code of length kmn . Moreover the Lee weight distribution of \mathcal{C} is the same as the Hamming weight distribution of $\phi_{km}(\mathcal{C})$.*

Consider the projections

$$\begin{aligned}\pi_v &: R_{k,m} \rightarrow R_{k,1} \text{ defined by } v \mapsto 0, \\ \pi_u &: R_{k,1} \rightarrow \mathbb{F}_2 \text{ defined by } u \mapsto 0,\end{aligned}$$

then $\mu = \pi_u \circ \pi_v$ is a projection from $R_{k,m}$ to \mathbb{F}_2 . The projections preserve orthogonality and projection of a free self-dual code is self-dual. The code \mathcal{D} is said to be a lift of \mathcal{C} if its projection is \mathcal{C} . The following theorem gives a bound for the minimum distance of a lift;

Theorem 2.4. [19] *Let \mathcal{C} be a linear code over $R_{k,m}$ of length n with minimum Lee weight d and $\mu(\mathcal{C})$ be its projection to \mathbb{F}_2 . If d' denotes the minimum Hamming weight of $\mu(\mathcal{C})$, we have $d \leq 2md'$.*

3. QUADRATIC DOUBLE CIRCULANT CODES OVER $R_{k,m}$

Double circulant codes are a subfamily of quasi-cyclic codes. Double circulant constructions are an effective method to form self-dual codes. On the other hand, quadratic residue codes is another topic of interest. In 2002, Gaborit defined quadratic double circulant (QDC) codes as a generalization of quadratic residue codes in [8]. In this section, we study QDC codes over $R_{k,m}$.

Let p be an odd prime and $Q_p(a, b, c)$ be the circulant matrix with first row r based on quadratic residues modulo p defined as $r[1] = a$, $r[i+1] = b$ if i is a quadratic residue and $r[i+1] = c$ if i is a quadratic non-residue modulo p . We state the special case of the main theorem from [8] where p is an odd prime;

Theorem 3.1. ([8]) *Let p be an odd prime and let $Q_p(a, b, c)$ be the circulant matrix with a, b and c as the elements of the ring $R_{k,m}$. If $p = 4k + 1$ then*

$$\begin{aligned}(3.1) \quad & Q_p(a, b, c) Q_p(a, b, c)^T \\ &= Q_p(a^2 + 2k(b^2 + c^2), 2ab - b^2 + k(b+c)^2, 2ac - c^2 + k(b+c)^2).\end{aligned}$$

If $p = 4k + 3$ then

$$\begin{aligned}(3.2) \quad & Q_p(a, b, c) Q_p(a, b, c)^T \\ &= Q_p(a^2 + (2k+1)(b^2 + c^2), ab + ac + k(b^2 + c^2) + (2k+1)bc, \\ &\quad ab + ac + k(b^2 + c^2) + (2k+1)bc).\end{aligned}$$

Definition 3.2. ([8]) The code generated by $P_p(a, b, c) = \begin{pmatrix} I_p & Q_p(a, b, c) \end{pmatrix}$ over $R_{k,m}$ is called a quadratic double circulant code and is denoted by $\mathcal{QDC}_p(R_{k,m})(a, b, c)$.

Example 3.3. Consider the code $\mathcal{QDC}_p(R_{2,2})(1+v+uv, u, v)$ that is generated by

$$\left[\begin{array}{c|ccccc} I_5 & 1+v+uv & u & v & v & u \\ & u & 1+v+uv & u & v & v \\ & v & u & 1+v+uv & u & v \\ & v & v & u & 1+v+uv & u \\ & u & v & v & u & 1+v+uv \end{array} \right].$$

Self-duality of the code is easily checked by Theorem 3.1. Moreover, each row of the generator matrix has Lee weight 8, which means the binary image of the code is doubly-even. It is an extremal self-dual $[40, 20, 8]$ code with partial weight distribution $1 + 285z^8 + 21280z^{12} + \dots$.

In the following, we define a special subfamily of units and non-units in $R_{k,m}$;

Definition 3.4. An element r of $R_{k,m}$ is called a *basic non-unit* if $r^2 = 0$ and a *basic unit* if $r^2 = 1$.

It is easily observed that $1 + r$ is a basic unit if and only if r is a basic non-unit.

In the following theorems families of self-dual QDC codes over $R_{k,m}$ are given.

Theorem 3.5. Let a be an element of $R_{k,m}$ such that $a^3 = 0$ and p be a prime with $p \equiv 3 \pmod{8}$ then the codes

$$\mathcal{QDC}_p(R_{k,m})(a, 1, a + a^2) \text{ and } \mathcal{QDC}_p(R_{k,m})(a, 1 + a^2, a + a^2)$$

are self-dual. The constructions are called I and II, respectively.

Proof. Since $p = 8k + 3$, $a^3 = 0$ and $\text{char}(R_{k,m}) = 2$, by the equation 3.2 we have

$$\begin{aligned} & Q_p(a, 1, a + a^2) Q_p(a, 1, a + a^2)^T \\ &= Q_p(a^2 + 1 + (a + a^2)^2, a + a(a + a^2) + (a + a^2), a + a(a + a^2) + (a + a^2)) \\ &= Q_p(0, 1, 1) = I_p, \end{aligned}$$

which implies that $\mathcal{QDC}_p(R_{k,m})(a, 1, a + a^2)$ is self-dual. By analogous steps $\mathcal{QDC}_p(R_{k,m})(a, 1 + a^2, a + a^2)$ is also self-dual. \square

The characterization of non-units given in Definition 3.4 can be used to construct self-dual codes as follows;

Theorem 3.6. Let a and b be two basic non-units in $R_{k,m}$ and p be a prime then the code $\mathcal{QDC}_p(R_{k,m})(1 + a, a, b)$ is self-dual whenever $p \equiv 1 \pmod{4}$. Moreover, $\mathcal{QDC}_p(R_{k,m})(a, 1 + b, a)$ is self-dual if $ab = 0$ and $p \equiv 3 \pmod{8}$. The constructions are called as III and IV, respectively.

Proof. Let $p = 4k + 1$ be a prime, a and b be basic non-units in $R_{k,m}$ then by equation 3.1

$$\begin{aligned} & Q_p(1 + a, a, b) Q_p(1 + a, a, b)^T \\ &= \begin{cases} Q_p((1 + a)^2, a^2, b^2) & \text{if } k \text{ is even} \\ Q_p((1 + a)^2, b^2, a^2) & \text{if } k \text{ is odd} \end{cases} \\ &= Q_p(1, 0, 0) = I_p. \end{aligned}$$

Hence, the code $\mathcal{QDC}_p(R_{k,m})(1 + a, a, b)$ is self-dual.

Let $p = 8k + 3$, a and b be basic non-units in $R_{k,m}$ with $ab = 0$. Then, since $\text{char}(R_{k,m}) = 2$, by equation 3.2 we have

$$\begin{aligned} & Q_p(a, 1 + b, a) Q_p(a, 1 + b, a)^T \\ &= Q_p(1, a(1 + b) + (1 + b)a, a(1 + b) + (1 + b)a) \\ &= Q_p(1, 0, 0) = I_p. \end{aligned}$$

Therefore, the code $\mathcal{QDC}_p(R_{k,m})(a, 1 + b, a)$ is self-dual. \square

We list some good QDC codes over $R_{k,m}$ in Table 1.

TABLE 1. Some examples of self-dual QDC codes over $R_{k,m}$

R	p	Construction	$a, (b)$	The binary image	Comment
$R_{2,1}$	5	III	$u, 0$	$[20, 10, 4]$	extremal
$R_{2,2}$	5	III	u, v	$[40, 20, 8]$	extremal singly-even
$R_{2,2}$	5	III	$u + uv, v$	$[40, 20, 8]$	extremal doubly-even
$R_{2,1}$	11	I, II	u	$[44, 22, 8]$	extremal
$R_{3,1}$	11	I	u	$[66, 33, 12]$	extremal
$R_{3,1}$	11	II	u	$[66, 33, 12]$	extremal
$R_{2,2}$	11	II	uv	$[88, 44, 12]$	singly-even
$R_{2,2}$	11	IV	u, uv	$[88, 44, 12]$	doubly-even
$R_{4,1}$	11	I	u^3	$[88, 44, 12]$	singly-even
$R_{3,1}$	19	I	u	$[114, 57, 16]$	-
$R_{3,2}$	11	II	$v + uv$	$[132, 66, 12]$	-
$R_{4,1}$	19	I	u^3	$[152, 76, 16]$	singly-even

4. CONSTRUCTIONS FOR SELF-DUAL CODES OVER $R_{k,m}$ BY λ -CIRCULANT MATRICES

In this section, the four circulant construction is generalized to λ -circulant matrices. Extremal singly-even binary self-dual codes of length 64 are constructed as Gray images of four circulant codes over \mathbb{F}_2 and $R_{2,2}$. The codes are going to be used in Section 5 to construct new binary self-dual codes of lengths 66 and 68.

The possible weight enumerators of singly-even extremal self-dual codes of length 64 are characterized in [4] as:

$$W_{64,1} = 1 + (1312 + 16\beta)y^{12} + (22016 - 64\beta)y^{14} + \dots \text{ where } 14 \leq \beta \leq 104,$$

$$W_{64,2} = 1 + (1312 + 16\beta)y^{12} + (23040 - 64\beta)y^{14} + \dots \text{ where } 0 \leq \beta \leq 277.$$

Recently, codes with $\beta = 29, 39, 53$ and 60 in $W_{64,1}$ and codes with $\beta = 51, 58$ in $W_{64,2}$ are constructed in [22] and a code with $\beta = 80$ in $W_{64,2}$ is constructed in [9]. Together with these the existence of such codes is now known for $\beta = 14, 18, 22, 25, 29, 32, 36, 39, 44, 46, 53, 60, 64$ in $W_{64,1}$ and for $\beta = 0, 1, 2, 4, 5, 6, 8, 9, 10, 12, 13, 14, 16, 17, 18, 20, 21, 22, 23, 24, 25, 28, 29, 30, 32, 33, 36, 37, 38, 40, 41, 44, 48, 51, 52, 56, 58, 64, 72, 80, 88, 96, 104, 108, 112, 114, 118, 120, 184$ in $W_{64,2}$.

The four circulant construction was defined in [1].

Definition 4.1. Let $r = (r_1, r_2, \dots, r_n)$ be an element of $(R_{k,m})^n$. The λ -cyclic shift of r is defined as $\sigma_\lambda(r) = (\lambda r_n, r_1, r_2, \dots, r_{m-1})$ where $\lambda \in R$. A square matrix is called λ -circulant if every row is the λ -cyclic shift of the previous one.

Since λ -circulant matrices commute with each other the four circulant construction can be extended to λ -circulant matrices. We have the following result:

Theorem 4.2. Let \mathcal{C} be the linear code over $R_{k,m}$ of length $4n$ generated by the four circulant matrix

$$G := \left[I_{2n} \mid \begin{array}{cc} A & B \\ B^T & A^T \end{array} \right]$$

where A and B are λ -circulant $n \times n$ matrices over $R_{k,m}$ satisfying $AA^T + BB^T = I_n$. Then the code \mathcal{C} is called a λ -four circulant code over $R_{k,m}$. The code \mathcal{C} and its binary image are self-dual.

Four circulant codes of length 32 over $R_{2,1}$ have been studied extensively in [9] and the codes with weight enumerators $\beta = 0, 16, 32, 48$ and 80 in $W_{64,2}$ were obtained. The code with the weight enumerator $\beta = 80$ in $W_{64,2}$ is the first such code in literature. For further reference we name this code as $\mathcal{C}_{64,80}$ which is the four circulant code over $R_{2,1}$ with

$$r_A = (u, 0, 0, 0, u, 1, u, 1 + u) \text{ and } r_B = (u, u, 0, 1, 1, 1 + u, 1 + u, 1 + u).$$

By considering $(1 + u)$ -four circulant codes of length 32 over $R_{2,1}$ we were able to obtain the binary codes with weight enumerators for $\beta = 8k$ in $W_{64,2}$ where $0 \leq k \leq 9$. These are listed in Table 2.

TABLE 2. $(1 + u)$ -four circulant codes over $R_{2,1}$

\mathcal{L}_i	r_A	r_B	β in $W_{64,2}$	$ Aut(\mathcal{L}_i) $
\mathcal{L}_1	$(u333uuu0)$	(11311010)	8	2^5
\mathcal{L}_2	$(u111000u)$	$(11333u1u)$	24	2^5
\mathcal{L}_3	$(u131u0uu)$	(31313030)	72	2^5
\mathcal{L}_4	$(33uu3110)$	$(113u00u3)$	0	2^5
\mathcal{L}_5	$(330u3110)$	$(1310uuu1)$	16	2^5
\mathcal{L}_6	$(33uu3130)$	$(331u0u01)$	32	2^5
\mathcal{L}_7	$(11u03130)$	$(131u0003)$	48	2^5
\mathcal{L}_8	$(310u113u)$	$(1330uu03)$	64	2^6
\mathcal{L}_9	$(u1110u3u)$	$(30u03113)$	8	2^5
\mathcal{L}_{10}	$(0133uu30)$	(10001113)	24	2^5
\mathcal{L}_{11}	$(u111001u)$	$(3u0u1311)$	40	2^5
\mathcal{L}_{12}	$(0133u01u)$	(10001311)	56	2^5

In order to construct extremal binary self-dual codes of length 64 as Gray images of λ -four circulant codes of length 16 over $R_{2,2}$ we lift binary codes to codes over $R_{2,1}$ and then lift these to codes over $R_{2,2}$. Theorem 2.4 tells us the minimum distance of the codes to be lifted. We demonstrate this in the following example;

Example 4.3. Let \mathcal{C} be the four circulant code of length 16 over \mathbb{F}_2 with $r_A = (1, 0, 0, 0)$ and $r_B = (1, 1, 1, 1)$. Then \mathcal{C} is a singly-even $[16, 8, 4]$ code. The code \mathcal{C} is lifted to \mathcal{C}' , which is the $(1 + u)$ -four circulant code of length 16 over $R_{2,1}$ with $r'_A = (1, 0, u, u)$ and $r'_B = (1, 1 + u, 1, 1 + u)$. The binary image $\phi_{21}(\mathcal{C}')$ of \mathcal{C}' is a self-dual $[32, 16, 6]$ code. Then \mathcal{C}' is lifted to the \mathcal{C}'' that is the $(1 + u + v + uv)$ -four circulant code of length 16 over $R_{2,2}$ with

$$r''_A = (1, 0, u, u + v + uv) \text{ and } r''_B = (1 + v + uv, 1 + u, 1 + v, 1 + u + v).$$

The binary code $\phi_{22}(\mathcal{C}'')$ is an extremal singly-even binary self-dual code of length 64 with weight enumerator $\beta = 0$ in $W_{64,2}$. Note that, $\pi_v(\mathcal{C}'') = \mathcal{C}'$, $\pi_u(\mathcal{C}') = \mathcal{C}$ and $\mu(\mathcal{C}'') = \mathcal{C}$.

In order to fit the upcoming tables we use hexadecimal number sytem. The one-to-one correspondence between hexadecimals and binary 4 tuples is as follows:

$$\begin{aligned} 0 &\leftrightarrow 0000, 1 \leftrightarrow 0001, 2 \leftrightarrow 0010, 3 \leftrightarrow 0011, \\ 4 &\leftrightarrow 0100, 5 \leftrightarrow 0101, 6 \leftrightarrow 0110, 7 \leftrightarrow 0111, \\ 8 &\leftrightarrow 1000, 9 \leftrightarrow 1001, A \leftrightarrow 1010, B \leftrightarrow 1011, \\ C &\leftrightarrow 1100, D \leftrightarrow 1101, E \leftrightarrow 1110, F \leftrightarrow 1111. \end{aligned}$$

To express elements of $R_{2,2}$ we use the ordered basis $\{uv, v, u, 1\}$. For instance $1+u+uv$ in $R_{2,2}$ is expressed as 1011 which is B . By considering λ -four circulant codes of length 16 over $R_{2,2}$ we obtain self-dual binary codes with weight enumerators in $W_{64,2}$ for various values for β , these are listed in Table 3.

TABLE 3. Self-dual λ -four circulant codes over $R_{2,2}$

\mathcal{M}_i	λ	r_A	r_B	β in $W_{64,2}$	$ Aut(\mathcal{M}_i) $
\mathcal{M}_1	3	$(F, 0, E, 2)$	$(7, 5, 3, D)$	0	2^5
\mathcal{M}_2	3	$(7, 0, C, A)$	$(F, F, 9, 5)$	16	2^5
\mathcal{M}_3	3	$(3, 0, D, 4)$	$(E, 3, F, B)$	48	2^5
\mathcal{M}_4	7	$(B, 0, 1, C)$	$(9, B, 1, 2)$	5	2^3
\mathcal{M}_5	7	$(B, 0, 1, 4)$	$(A, 7, 5, F)$	8	2^4
\mathcal{M}_6	7	$(3, 0, 7, A)$	$(B, C, D, 9)$	9	2^3
\mathcal{M}_7	7	$(7, 0, 5, C)$	$(1, 3, 2, 5)$	12	2^4
\mathcal{M}_8	7	$(D, 0, F, C)$	$(F, 1, 7, A)$	13	2^3
\mathcal{M}_9	7	$(B, 0, 1, C)$	$(A, 5, 5, D)$	16	2^5
\mathcal{M}_{10}	7	$(B, 0, F, A)$	$(B, C, D, 7)$	17	2^3
\mathcal{M}_{11}	7	$(7, 0, 5, C)$	$(2, 7, 5, F)$	24	2^4
\mathcal{M}_{12}	F	$(1, 0, 2, E)$	$(D, 3, 5, 7)$	0	2^5
\mathcal{M}_{13}	F	$(C, 0, 3, 6)$	$(1, B, 7, 1)$	16	2^5
\mathcal{M}_{14}	F	$(F, 0, B, A)$	$(F, B, 4, 5)$	48	2^5
\mathcal{M}_{15}	B	$(9, 0, F, C)$	$(B, 6, 9, 3)$	5	2^3
\mathcal{M}_{16}	B	$(D, 0, 3, C)$	$(6, B, 5, 3)$	8	2^4
\mathcal{M}_{17}	B	$(5, 0, B, 4)$	$(7, 6, D, 9)$	9	2^3
\mathcal{M}_{18}	B	$(5, 0, 1, E)$	$(9, 9, C, B)$	12	2^4
\mathcal{M}_{19}	B	$(D, 0, 1, 6)$	$(F, 1, 7, C)$	13	2^3
\mathcal{M}_{20}	B	$(5, 0, B, C)$	$(E, D, F, 5)$	16	2^3
\mathcal{M}_{21}	B	$(B, 0, 5, C)$	$(7, E, D, 7)$	17	2^3
\mathcal{M}_{22}	B	$(D, 0, 3, 4)$	$(E, 9, 3, 1)$	24	2^4

Remark 4.4. In order to construct the codes in Table 2 the binary four circulant codes are lifted to $R_{2,1}$. Similarly, to construct the codes in Table 3 the binary four circulant codes are lifted to $R_{2,1}$ and then to $R_{2,2}$. This reduces the search field remarkably from $2^{32} = 4294967296$ to $2^{16} = 65536$.

5. NEW BINARY SELF-DUAL CODES BY EXTENSIONS

By applying the extension theorems to the self-dual codes constructed in Section 4 we were able to obtain new binary self-dual codes of lengths 66 and 68. In particular we were able to construct 11 new codes of length 66 and 34 new codes

of length 68. Extensions for self-dual codes were first used by Brualdi and Pless in [3]. Since then different versions of extensions applied, for some of these we refer to [12, 6] and [16]. The following extension theorems hold for any commutative Frobenius ring R of characteristic 2.

Theorem 5.1. ([6]) *Let \mathcal{C} be a self-dual code over R of length n and $G = (r_i)$ be a $k \times n$ generator matrix for \mathcal{C} , where r_i is the i -th row of G , $1 \leq i \leq k$. Let c be a unit in R such that $c^2 = 1$ and X be a vector in R^n with $\langle X, X \rangle = 1$. Let $y_i = \langle r_i, X \rangle$ for $1 \leq i \leq k$. Then the following matrix*

$$\left(\begin{array}{cc|c} 1 & 0 & X \\ \hline y_1 & cy_1 & r_1 \\ \vdots & \vdots & \vdots \\ y_k & cy_k & r_k \end{array} \right),$$

generates a self-dual code \mathcal{C}' over R of length $n + 2$.

A more specific extension method which can be applied to generator matrices in standard form is as follows:

Theorem 5.2. ([16]) *Let \mathcal{C} be a self-dual code generated by $G = (I_n | A)$ over R . If the sum of the elements in i -th row of A is r_i then the matrix:*

$$G^* = \left(\begin{array}{cc|cccccc} 1 & 0 & x_1 & \dots & x_n & 1 & \dots & 1 \\ \hline y_1 & cy_1 & & & & & & \\ \vdots & \vdots & & & & & & \\ y_n & cy_n & & & I_n & & A & \end{array} \right),$$

where $y_i = x_i + r_i$, c is a unit with $c^2 = 1$, $X = (x_1, \dots, x_n)$ and $\langle X, X \rangle = 1 + n$, generates a self-dual code \mathcal{C}^ over R .*

5.1. \mathbb{F}_2 -extensions. The Gray images of the codes in tables 2 and 3 are extremal singly-even self-dual binary codes of length 64. In this section, we construct extremal binary self-dual codes of length 66 by applying Theorem 5.1. Eleven new codes are obtained.

We recall that a self-dual $[66, 33, 12]_2$ -code has a weight enumerator in one of the following forms [5];

$$W_{66,1} = 1 + (858 + 8\beta)y^{12} + (18678 - 24\beta)y^{14} + \dots \text{ where } 0 \leq \beta \leq 778,$$

$$W_{66,2} = 1 + 1690y^{12} + 7990y^{14} + \dots$$

$$\text{and } W_{66,3} = 1 + (858 + 8\beta)y^{12} + (18166 - 24\beta)y^{14} + \dots \text{ where } 14 \leq \beta \leq 756,$$

Recently, five new codes in $W_{66,1}$ are constructed in [9]. The existence of such codes is known for $\beta = 0, 1, 2, 3, 5, 6, 8, \dots, 11, 14, \dots, 18, 20, \dots, 54, 56, 59, 60, 62, \dots, 69, 71, \dots, 74, 76, 77, 78, 80, 83, 84, 86, 87, 92, 94$ in $W_{66,1}$. For a list of known codes in $W_{66,3}$ we refer to [10].

We construct the codes with weight enumerators $\beta = 19, 61, 75, 79, 81, 82, 85, 88, 89, 90$ and 100 in $W_{66,1}$. The extension in Theorem 5.1 is applied to the binary images of the codes constructed in Section 4 to obtain the new codes. The results are given in Table 4 where $\mathbf{1}^{32}$ denotes 32 successive 1s in X .

TABLE 4. New extremal binary self-dual codes with weight enumerators in $W_{66,1}$ by Theorem 5.1 (11 codes)

Code	The extension vector X	β in $W_{66,1}$
\mathcal{M}_{17}	101010101110011100100011011100101 ³²	19
\mathcal{M}_3	11001100001011100111100101011111 ³²	61
\mathcal{L}_8	100010111111110110110101101001001 ³²	75
\mathcal{L}_8	00010101001111110101110111100101 0111100111001000011111001100000	79
\mathcal{L}_3	01100110100001001100000110100000 01001101100110110111110101111001	81
\mathcal{L}_8	01010110111110101100011010100111 00010101100101110100110101101001	82
\mathcal{L}_3	00111101100000000111010010101001 0010000111000011110001100010100	85
$\mathcal{C}_{64,80}$	111000001010110101111001001101101 ³²	88
$\mathcal{C}_{64,80}$	101001000011101011101001110000011 ³²	89
$\mathcal{C}_{64,80}$	000111111101111011110011100010111 ³²	90
$\mathcal{C}_{64,80}$	111000011000000000010000100110111 ³²	100

5.2. $R_{2,1}$ -extensions. In this section, we obtain new extremal binary self-dual codes of length 68 by considering $R_{2,1}$ -extensions of the codes constructed in the previous section. The ring $R_{2,2}$ can be considered as an extension of $R_{2,1}$. Throughout this section, φ_u is the Gray map from $R_{2,2}$ to $R_{2,1}$ defined as $\varphi_u(a + bv) = (b, a + b)$ where $a, b \in R_{2,1}$. We consider the extensions of the codes in Table 2 as well as the Gray images of the codes in Table 3 under φ_u . 39 new extremal binary self-dual codes of length 68 are obtained as the binary images of the extensions.

The weight enumerator of an extremal binary self-dual code of length 68 is characterized in [5] as follows:

$$\begin{aligned}
W_{68,1} &= 1 + (442 + 4\beta)y^{12} + (10864 - 8\beta)y^{14} + \dots, \quad 104 \leq \beta \leq 1358, \\
W_{68,2} &= 1 + (442 + 4\beta)y^{12} + (14960 - 8\beta - 256\gamma)y^{14} + \dots
\end{aligned}$$

where $0 \leq \gamma \leq 11$ and $14\gamma \leq \beta \leq 1870 - 32\gamma$. Tsai et al. constructed new extremal self-dual binary codes of lengths 66 and 68 in [20]. Recently, 3 codes with previously unknown weight enumerators in $W_{68,1}$ were constructed in [14]. Together with the codes obtained in [20, 14] the existence of codes in $W_{68,1}$ are known for $\beta = 104, 117, 120, 122, 123, 125, \dots, 168, 170, \dots, 232, 234, 235, 236, 241, 255, 257, \dots, 269, 302, 328, \dots, 336, 338, 339, 345, 347, 355, 401$.

We obtain a code with a weight enumerator $\beta = 169$ in $W_{68,1}$.

First codes with $\gamma = 4$ and $\gamma = 6$ in $W_{68,2}$ are constructed in [11]. Recently, new codes in $W_{68,2}$ are obtained in [16, 13, 14] together with these, codes exist for

$W_{68,2}$ when

$$\begin{aligned}
\gamma &= 0, \beta = 44, \dots, 154 \text{ or } \beta \in \{2m | m = 19, 20, 88, 102, 119, 136 \text{ or } 78 \leq m \leq 86\}; \\
\gamma &= 1, \beta = 49, 57, 59, \dots, 160 \text{ or } \beta \in \{2m | m = 27, 28, 29, 95, 96 \text{ or } 81 \leq m \leq 89\}; \\
\gamma &= 2, \beta = 65, 68, 69, 71, 77, 81, 159 \text{ or } \beta \in \{2m | 37 \leq m \leq 68, 70 \leq m \leq 81\} \text{ or} \\
&\beta \in \{2m + 1 | 42 \leq m \leq 69, 71 \leq m \leq 77\}; \\
\gamma &= 3, \beta = 101, 117, 123, 127, 133, 137, 141, 145, 147, 149, 153, 159, 193 \text{ or} \\
&\beta \in \{2m | m = 44, 45, 48, 50, 51, 52, 54, \dots, 58, 61, 63, \dots, 66, 68, \dots, 72, 74, 77, \dots, 81, 88, 94, 98\}; \\
\gamma &= 4, \beta \in \{2m | m = 51, 55, 58, 60, 61, 62, 64, 65, 67, \dots, 71, 75, \dots, 78, 80\} \text{ and} \\
\gamma &= 6 \text{ with } \beta \in \{2m | m = 69, 77, 78, 79, 81, 88\}.
\end{aligned}$$

In this section, we construct the codes with weight enumerators in $W_{68,2}$ for $\gamma = 0$ and $\beta = 178$; $\gamma = 1$ and $\beta = 180$; $\gamma = 2$ and $\beta = 60, 62, 64, 66, 70, 72, 164, 166, 168, 170, 172, 174, 176, 178, 180, 182, 186$; $\gamma = 3$ and $\beta = 94, 107, 118, 120, 156, 168, 172, 180$; $\gamma = 4$ and $\beta = 98, 104, 108, 112, 174, 194$.

By considering $R_{2,1}$ -extensions of codes in Table 2 with respect to Theorem 5.2 we were able to obtain 14 new extremal binary self-dual codes, which are listed in Table 5.

TABLE 5. New codes in $W_{68,2}$ by Theorem 5.2 on $R_{2,1}$ (14 codes)

\mathcal{L}_i	X	c	γ	β
\mathcal{L}_4	(1313uu0133130u11)	$1 + u$	2	60
\mathcal{L}_4	(1131uu011133u011)	1	2	62
\mathcal{L}_4	(0001u11uu3110300)	1	2	64
\mathcal{L}_4	(00u1u130u111u1u0)	$1 + u$	2	66
\mathcal{L}_4	(uuu30330013101uu)	$1 + u$	2	70
\mathcal{L}_4	(u0u1u13uu333u3u0)	$1 + u$	2	72
\mathcal{L}_3	(u3000uu33u31u031)	1	2	166
\mathcal{L}_3	(u1u0u0u11u31uu13)	$1 + u$	2	170
\mathcal{L}_3	(03u0u00330310u31)	$1 + u$	2	172
\mathcal{L}_3	(u1uuu0u11u31u013)	$1 + u$	2	174
\mathcal{L}_3	(01000u0110310013)	$1 + u$	2	176
\mathcal{L}_3	(011300u031111313)	1	3	156
\mathcal{L}_3	(3u131011301u0u10)	$1 + u$	3	172
\mathcal{L}_3	(103130333010u010)	$1 + u$	3	180

Example 5.3. Let \mathcal{C} be the code obtained by applying Theorem 5.1 for $\varphi_u(M_4)$ over $R_{2,1}$ with

$$X = (u, 1 + u, 0, 0, 0, 1 + u, 0, 0, 1, u, 0, 1, u, u, 1 + u, 0, 1111111111111111)$$

and $c = 1 + u$ then the binary image of the extension is an extremal binary self-dual code of length 68 with a weight enumerator $\beta = 169$ in $W_{68,1}$. The code \mathcal{C} is the first extremal binary self-dual code with this weight enumerator.

Theorem 5.1 is applied to codes in Table 2 and $R_{2,1}$ -images of codes in Table 3. 24 new extremal binary self-dual codes of length 68 are obtained as Gray

images of the extensions. Similar to Section 4 lifts can be applied to the extensions. If X is a possible extension vector for a free self-dual code \mathcal{C} over $R_{2,1}$ then $\pi_u(X)$ is an extension vector for $\pi_u(\mathcal{C})$. In order to extend \mathcal{C} we may lift an extension vector for $\pi_u(\mathcal{C})$. Theorem 2.4 gives an idea on which extension vectors to lift. For instance, a possible extension vector for the binary code $\pi_u(\varphi_u(M_{12}))$ is (00010111001100110000001000110011). By considering the lifts of this vector we were able to obtain new codes with weight enumerators corresponding to rare parameters $\gamma = 4$ and $\beta = 86, 96$ and 98 . Those are listed in Table 6. Considering lifts reduces the workload remarkably from 4^{32} to 2^{32} .

TABLE 6. New codes in $W_{68,2}$ by Theorem 5.1 on $R_{2,1}$ (24 codes)

Code	X	c	γ	β
\mathcal{L}_3	(31u1u11133u10u113u10u33013010111)	$1+u$	0	178
\mathcal{L}_3	(10u1u033uu3u00u03101010uu10u3u0u)	1	1	180
\mathcal{L}_{12}	(11330u11u1103101u3u3101u31uu33u)	1	2	164
\mathcal{L}_8	(0uuu0011113u13u01303113033311003)	1	2	168
\mathcal{L}_8	(00000031313033u031u3333u33311003)	$1+u$	2	178
\mathcal{L}_8	(u0uuu033111033uu1301113u13331uu1)	1	2	180
\mathcal{L}_8	(u0u00011313u31u011u1113u33313u01)	1	2	182
\mathcal{L}_3	(u3uuu33uu10uu00103010u001u030u13)	$1+u$	2	186
$\varphi_u(M_{12})$	(13331031u0u1133u111111111111111)	1	3	94
$\varphi_u(M_4)$	(11u301u33u0133u3u1u3u0uu010330uu)	1	3	107
$\varphi_u(M_{12})$	(11333u3100u1133u1331133313313133)	$1+u$	3	118
$\varphi_u(M_{17})$	(1310u30u33010000111111111111111)	$1+u$	3	120
\mathcal{L}_3	(uuu310u11u3u00u1uuu303u3u3u13333)	1	3	164
\mathcal{L}_3	(uu031u03103u0u01u00103u3u1u13111)	$1+u$	3	166
\mathcal{L}_3	(uuu11u031u3u0u01u003u3u303u31131)	$1+u$	3	168
\mathcal{L}_3	(u0031003301uuuu3u001u103u3u31331)	$1+u$	3	174
$\varphi_u(M_{12})$	(000101330011uu330u000u1u0011uu33)	$1+u$	4	86
$\varphi_u(M_{12})$	(uu01u1110u33u033uu0u003u0u31u013)	$1+u$	4	96
$\varphi_u(M_{12})$	(0001u3130u31uu1100uuu1uu0130u31)	$1+u$	4	98
$\varphi_u(M_{12})$	(u3u3u1110u3310u311111111111111)	1	4	104
$\varphi_u(M_{12})$	(u3010333003110031331133333113313)	1	4	108
$\varphi_u(M_{12})$	(u1u10313001110u33313331111331111)	1	4	112
\mathcal{L}_8	(00u00u33111u130011u31130111310u3)	$1+u$	4	174
\mathcal{L}_8	(u300033003u0uuu10303000u1uu10u31)	1	4	194

Remark 5.4. The binary generator matrices of the new extremal binary self-dual codes of lengths 66 and 68 that are constructed in tables 4, 5 and 6 are available online at [15].

Acknowledgements

The authors would like to thank Bahattin Yıldız for his valuable comments.

REFERENCES

- [1] K. Betsumiya, S. Georgiou, T.A. Gulliver, M. Harada and C. Koukouvinos, “On self-dual codes over some prime fields”, *Discrete Math*, vol 262, pp. 37–58, 2003.

- [2] W. Bosma, J. Cannon and C. Playoust, “The Magma algebra system. I. The user language”, *J. Symbolic Comput.*, vol. 24, pp. 235–265, 1997.
- [3] R. A. Brualdi and V. S. Pless, “Weight enumerators of self-dual codes”, *IEEE Trans. Inform. Theory*, Vol. 37, pp. 1222–1225, 1991.
- [4] J. H. Conway, N. J. A. Sloane, “A new upper bound on the minimal distance of self-dual codes”, *IEEE Trans. Inform. Theory*, Vol. 36, 6, 1319–1333, 1990.
- [5] S. T. Dougherty, T. A. Gulliver, M., Harada, “Extremal binary self dual codes”, *IEEE Trans. Inform. Theory*, Vol. 43 pp. 2036–2047, 1997.
- [6] S.T. Dougherty, J.L. Kim, H. Kulosman and H. Liu, “Self-dual codes over commutative Frobenius rings”, *Finite Fields Appl.*, Vol.16, pp.14–26, 2010.
- [7] S.T. Dougherty, B. Yildiz and S. Karadeniz, “Codes over R_k , Gray Maps and their Binary Images”, *Finite Fields Appl.*, Vol. 17, pp. 205–219, 2011.
- [8] P. Gaborit, “Quadratic double circulant codes over fields”, *Journal of Combinatorial Theory Series A*, Vol. 97, Issue 1, pp. 85–107, 2002.
- [9] S. Karadeniz, B. Yildiz and N. Aydın, “Extremal binary self-dual codes of lengths 64 and 66 from four-circulant constructions over codes $\mathbb{F}_2 + u\mathbb{F}_2$ ”, *FILOMAT*, Vol. 28, Issue 5, pp. 937–945, 2014.
- [10] S. Karadeniz and B. Yildiz, “New extremal binary self-dual codes of length 66 as extensions of self-dual code over R_k ”, *J. Franklin Inst.*, Vol. 350, no. 8, pp.1963–1973, 2013.
- [11] S. Karadeniz, B. Yildiz, “New extremal binary self-dual codes of length 68 from R_2 -lifts of binary self-dual codes”, *Advances in Mathematics of Communications*, Vol. 7, no. 2, pp. 219–229, 2013.
- [12] J.-L. Kim, “New extremal self-dual codes of lengths 36, 38 and 58”, *IEEE Trans. Inf. Theory*, Vol.47, No.1, pp.386–393, 2001.
- [13] A. Kaya, B. Yildiz, İ. Şiap, “New extremal binary self-dual codes from $\mathbb{F}_4 + u\mathbb{F}_4$ -lifts of quadratic double circulant codes over \mathbb{F}_4 ”, available online at <http://arxiv.org/abs/1405.7147>
- [14] A. Kaya, B. Yildiz, “New extremal binary self-dual codes of length 68”, *Journal of Algebra Combinatorics Discrete Structures and Applications*, Vol. 1, No. 1, pp 29–39, 2014.
- [15] A. Kaya, N. Tüfekçi, *Binary generator matrices of new extremal self-dual binary codes of lengths 66 and 68*, available online at <http://www.fatih.edu.tr/~akaya/newbinary66-68.html>
- [16] A. Kaya, B. Yildiz, “Extension theorems for self-dual codes over rings and new binary self-dual codes”, available online at <http://arxiv.org/abs/1404.0195>.
- [17] E. M. Rains, “Shadow Bounds for Self Dual Codes”, *IEEE Trans. Inf. Theory*, Vol.44, pp.134–139, 1998.
- [18] M. Shi, L. Chen “Construction of two-Lee weight codes over $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$ ”, *International Journal of Computer Mathematics*.
- [19] N. Tüfekçi, B. Yildiz, “On codes over $R_{k,m}$ and constructions for new binary self-dual codes”, to appear in *Mathematica Slovaca*.
- [20] H-P. Tsai, P-Y. Shih, R-Y. Wuh, W-K. Su, C-H. Chen, “Construction of self-dual codes”, *IEEE Trans. Inform. Theory*, Vol. 54, pp. 3826–3831, 2008.
- [21] J. Wood, “Duality for modules over finite rings and applications to coding theory”, *Amer. J. Math.*, Vol. 121, pp. 555–575, 1999.
- [22] N. Yankov, “Self-dual $[62, 31, 12]$ and $[64, 32, 12]$ codes with an automorphism of order 7”, *Advances in Mathematics of Communications*, Vol.8, No1. pp.73–81, 2014.
- [23] B. Yildiz, S. Karadeniz, “Linear Codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ ”, *Des. Codes Crypt.* vol.54, pp. 61–81, 2010.

DEPARTMENT OF MATHEMATICS, FATİH UNIVERSITY, 34500, İSTANBUL, TURKEY
E-mail address: akaya@fatih.edu.tr, nesibe.tufekci@fatih.edu.tr